

1 Claim 7 (original): The method according to Claim 1, wherein the selected resources are function
2 calls to functions of one or more executable programs.

1 Claim 8 (original): The method according to Claim 1, wherein the selected resources are
2 Enterprise JavaBeans ("EJBs") and the permitted actions are methods on the EJBs.

1 Claim 9 (original): The method according to Claim 1, wherein the selected resources are servlets
2 and the permitted actions are methods of the servlets.

1 Claim 10 (original): The method according to Claim 1, wherein the selected resources are
2 Uniform Resource Identifiers ("URIs") and the permitted actions are methods which reference the
3 URIs.

1 Claim 11 (original): The method according to Claim 1, wherein the selected resources are
2 JavaServer Pages ("JSPs") and the permitted actions are methods referenced from the JSPs.

1 Claim 12 (original): The method according to Claim 1, wherein the selected resources are any
2 resource that is expressible to the security system and the permitted actions are selected from a set
3 of actions that are permitted on those resources.

1 Claim 13 (original): The method according to Claim 1, further comprising the steps of:
2 receiving an access request for a particular one of the selected resources;

Serial No. 09/943,618

-5-

RSW920010125US1

Amendments to the Claims

1 Claim 1 (currently amended): A method of improving security policy administration and
2 enforcement using a role-permission model, comprising steps of:
3 identifying one or more groups of permitted actions on selected resources;
4 assigning a name to each identified group;
5 defining each assigned name to a security system as a security object; and
6 associating subjects with each assigned name.

1 Claim 2 (original): The method according to Claim 1, wherein the assigned name is a role name.

1 Claim 3 (original): The method according to Claim 1, wherein the selected resources are
2 executable methods.

1 Claim 4 (original): The method according to Claim 1, wherein the selected resources are columns
2 of a database table.

1 Claim 5 (original): The method according to Claim 1, wherein the selected resources are rows of
2 a database table.

1 Claim 6 (original): The method according to Claim 1, wherein the selected resources are files and
2 the permitted actions are file access operations.

Serial No. 09/943,618

-4-

RSW920010125US1

1 Claim 7 (original): The method according to Claim 1, wherein the selected resources are function
2 calls to functions of one or more executable programs.

1 Claim 8 (original): The method according to Claim 1, wherein the selected resources are
2 Enterprise JavaBeans ("EJBs") and the permitted actions are methods on the EJBs.

1 Claim 9 (original): The method according to Claim 1, wherein the selected resources are servlets
2 and the permitted actions are methods of the servlets.

1 Claim 10 (original): The method according to Claim 1, wherein the selected resources are
2 Uniform Resource Identifiers ("URIs") and the permitted actions are methods which reference the
3 URIs.

1 Claim 11 (original): The method according to Claim 1, wherein the selected resources are
2 JavaServer Pages ("JSPs") and the permitted actions are methods referenced from the JSPs.

1 Claim 12 (original): The method according to Claim 1, wherein the selected resources are any
2 resource that is expressible to the security system and the permitted actions are selected from a set
3 of actions that are permitted on those resources.

1 Claim 13 (original): The method according to Claim 1, further comprising the steps of:
2 receiving an access request for a particular one of the selected resources;

3 determining one or more roles which are required for accessing the particular resource;
4 determining an identity of a source of the access request;
5 for each of the required roles, until obtaining a successful result or exhausting the required
6 roles, determining whether the identity of the source is associated with the required role; and
7 authorizing access to the particular resource only if the successful result was obtained.

1 Claim 14 (original): The method according to Claim 13, wherein the step of determining the one
2 or more roles further comprises consulting a collection created from the identified permitted
3 actions on the particular resource.

1 Claim 15 (currently amended): A system for improving security policy administration and
2 enforcement in a computing network using a role-permission model, comprising:
3 means for identifying one or more groups of permitted actions on selected resources;
4 means for assigning a name to each identified group;
5 ~~means for defining each assigned name to a security system as a security object; and~~
6 means for associating subjects with each assigned name.

1 Claim 16 (original): The system according to Claim 15, further comprising:
2 means for receiving an access request for a particular one of the selected resources;
3 means for determining one or more roles which are required for accessing the particular
4 resource;
5 means for determining an identity of a source of the access request;

Serial No. 09/943,618

access request;

for each of the required roles, until obtaining a successful result or exhausting the required roles, computer readable program code means for determining whether the identity of the source is associated with the required role; and

computer readable program code means for authorizing access to the particular resource only if the successful result was obtained.

for each of the required roles, until obtaining a successful result or exhausting the required roles, means for determining whether the identity of the source is associated with the required role; and

means for authorizing access to the particular resource only if the successful result was obtained.

Claim 17 (currently amended): A computer program product for improving security policy administration and enforcement in a computing network using a role-permission model, the computer program product embodied on one or more computer readable media and comprising:

computer readable program code means for identifying one or more groups of permitted actions on selected resources;

computer readable program code means for assigning a name to each identified group;

~~computer readable program code means for defining each assigned name to a security system as a security object; and~~

computer readable program code means for associating subjects with each assigned name.

Claim 18 (original): The computer program product according to Claim 17, further comprising:

computer readable program code means for receiving an access request for a particular one of the selected resources;

computer readable program code means for determining one or more roles which are required for accessing the particular resource;

computer readable program code means for determining an identity of a source of the

7 access request;

8 for each of the required roles, until obtaining a successful result or exhausting the required
9 roles, computer readable program code means for determining whether the identity of the source
10 is associated with the required role; and

11 computer readable program code means for authorizing access to the particular resource
12 only if the successful result was obtained.